JP2000228674

Title:
ADDRESS ALLOCATING METHOD IN INTER-PLURAL POINT COMMUNICATION, COMMUNICATING METHOD AMONG PLURAL POINTS AND ITS CONNECTING DEVICE

Abstract:

PROBLEM TO BE SOLVED: To reduce the setting burden of 2nd point sides by allocating an address which is different from that of a destination terminal connected to a terminal in the 2nd points but common among all of the 2nd points. SOLUTION: 2nd points 200 respectively have an address converting part such as PROXY server and fire wall for converting the private address of a client machine 201 into a global address. In a network connecting plural points, connection destinations of communication data having the same connection destination address are divided by converting the connection destination address into the address of a connection destination terminal for the communication data on a communication path between one point to which the terminal to be a connection destination candidate belongs and a connection source. Thus, it is possible for the 2nd points 200 to easily and directly communicate with a network 1 and to construct a virtual private network(VPN).

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－228674
（P2000－228674A）
(43)公開日　平成12年８月15日(2000.8.15)

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｄ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28		11/20	Ｂ	９Ａ００１
12/66				

審査請求　未請求　請求項の数18　ＯＬ　（全 12 頁）

(21)出願番号　特願平11－27968

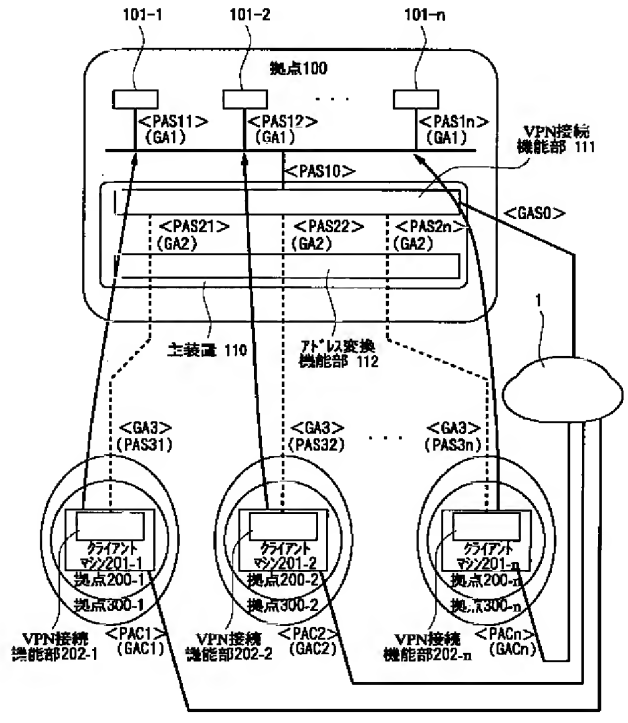
(22)出願日　平成11年２月４日(1999.2.4)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　岡田　浩一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　中山　隆二
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100069981
弁理士　吉田　精孝

最終頁に続く

(54)【発明の名称】　複数拠点間通信におけるアドレス割り当て方法及び複数拠点間の通信方法並びにその接続装置

(57)【要約】
【課題】　拠点間でプライベートアドレスが重複することなく、かつグローバルアドレスアドレスを大量消費することなく、複数拠点間の通信方法及び接続装置を提供する。
【解決手段】　複数の拠点間を接続したネットワークにおいて、接続先の候補となる端末が属する一の拠点と接続元との通信経路上の通信データに対して、その接続先アドレスを接続先端末のアドレスに変換することにより同一の接続先アドレスを有する通信データの接続先を振り分ける。



【特許請求の範囲】
【請求項１】　第１の拠点と複数の第２の拠点とがそれぞれＶＰＮ（VirtualPrivate Network）を介して接続されたネットワークにおける複数拠点間通信において、
前記第２の拠点では一の端末のみがＶＰＮ接続を行うとともに、この端末が第１の拠点における特定の端末と接続する場合には、
全ての第２の拠点におけるＶＰＮトンネルに付加される仮想インタフェイスに対して同一のアドレスを割り当てるとともに、第２の拠点における端末の接続先となる端末に対して前記アドレスとは異なるとともに全ての第２の拠点間で共通なアドレスを割り当てることを特徴とする複数拠点通信におけるアドレス割り当て方法。
【請求項２】　第１の拠点と第２の拠点とがそれぞれＶＰＮを介して接続されたネットワークにおける複数拠点間通信において、
前記第２の拠点を包含する第３の拠点内において未申請のグローバルアドレスが使用されておらず、この第２の拠点では一の端末のみが第１の拠点に対してＶＰＮ接続を行う場合には、
ＶＰＮ接続の際に、第２の拠点が新たに意識する第１の拠点内の端末に対して申請済みグローバルアドレスを別名アドレスとして割り当てることを特徴とする複数拠点間通信におけるアドレス割り当て方法。
【請求項３】　第１の拠点と第２の拠点間を接続したネットワークにおける複数拠点間の通信方法において、
接続先の候補となる端末が属する一の拠点と接続元との通信経路上の通信データであって同一の接続先アドレスを有する通信データに対して、その接続先アドレスを接続先端末のアドレスに変換することにより通信データの接続先を振り分けることを特徴とする複数拠点間の通信方法。
【請求項４】　第１の拠点と第２の拠点間を接続したネットワークにおける複数拠点間の通信方法において、
接続先の候補となる端末が属する一の拠点と接続元との通信経路上の通信データであって同一の接続先アドレスを有する通信データについて、該通信データの通信経路に基づき接続先を振り分けることを特徴とする複数拠点間の通信方法。
【請求項５】　第１の拠点と第２の拠点間を接続したネットワークにおける複数拠点間の通信方法において、
接続先の候補となる端末が属する一の拠点と接続元との通信経路上の通信データであって同一の接続先アドレスを有する通信データに対して、その接続先アドレスを、該通信データの通信経路に対応する接続先端末のアドレスに変換することにより通信データの接続先を振り分けることを特徴とする複数拠点間の通信方法。
【請求項６】　前記第１の拠点と第２の拠点間をＶＰＮで接続し、前記通信経路をＶＰＮトンネルとしたことを特徴とする請求項３～５何れか１項記載の複数拠点間の通信方法。
【請求項７】　前記アドレス変換では、請求項１又は請求項２記載の複数拠点通信におけるアドレス割り当て方法により割り当てたアドレスに基づき、ＶＰＮトンネルを通過する通信データの送信先又は送信元アドレスを変換することを特徴とする請求項６記載の複数拠点間の通信方法
【請求項８】　前記アドレス変換の際に用いる全ての別名アドレスを第１の拠点側で予め用意することを特徴とする請求項３又は５～７何れか１項記載の複数拠点間の通信方法。
【請求項９】　第２の拠点を複数の部分拠点に分離するとともに、各部分拠点から個別に第１の拠点に対してＶＰＮ接続を行うことを特徴とする請求項３～８何れか１項記載の複数拠点間の通信方法。
【請求項１０】　第１の拠点を経由することにより複数の第２の拠点間の通信を行うことを特徴とする請求項３～９何れか１項記載の複数拠点間の通信方法。
【請求項１１】　複数の拠点間を接続したネットワークにおける複数拠点間の接続装置であって、
接続先の候補となる端末が属する一の拠点と接続元との通信経路上の通信データに対して、その接続先アドレスを接続先端末のアドレスに変換することにより同一の接続先アドレスを有する通信データの接続先を振り分ける振り分け手段を有することを特徴とする複数拠点間の接続装置。
【請求項１２】　第１の拠点と第２の拠点とがそれぞれＶＰＮを介して接続されたネットワークにおいて第１の拠点とグローバルネットワークとを接続する接続装置であって、
ＶＰＮトンネル内を通過する通信データの送信元又は送信先アドレスをＶＰＮ接続ごとに変換するアドレス変換手段を有することを特徴とする複数拠点間の接続装置。
【請求項１３】　前記第２の拠点では一の端末のみがＶＰＮ接続を行うとともに、この端末が第１の拠点における特定の端末と接続する場合において、
全ての第２の拠点におけるＶＰＮトンネルに付加される仮想インタフェイスに対して同一のアドレスを割り当てるとともに、第２の拠点における端末の接続先となる端末に対して前記アドレスとは異なるとともに全ての第２の拠点間で共通なアドレスを割り当て、
前記アドレス変換手段はこのアドレスに基づき通信データのアドレスを変換することを特徴とする請求項１２記載の複数拠点間の接続装置。
【請求項１４】　第１の拠点と複数の第２の拠点とがそれぞれＶＰＮを介して接続されたネットワークにおいて第１の拠点とグローバルネットワークとを接続する接続装置であって、
前記第２の拠点では一の端末のみがＶＰＮ接続を行うとともに、この端末が第１の拠点における特定の端末と接

続する場合には、
全ての第２の拠点におけるＶＰＮトンネルに付加される仮想インタフェイスに対して同一のアドレスを割り当てるとともに、第２の拠点における端末の接続先となる端末に対して前記アドレスとは異なるとともに全ての第２の拠点間で共通なアドレスを割り当て、
ＶＰＮトンネルを通る通信データの送信先アドレス又は送信元アドレスとして前記アドレスを用いることを特徴とする複数拠点間の接続装置。
【請求項１５】　前記アドレスに基づきＶＰＮトンネル内を通過する通信データの送信元又は送信先アドレスをＶＰＮ接続ごとに変換するアドレス変換手段を有することを特徴とする請求項１４記載の複数拠点間の接続装置。
【請求項１６】　前記アドレス変換手段による変換されたアドレスに基づき接続先を振り分ける接続先振り分け手段を有することを特徴とする請求項１３又は１５何れか１項記載の複数拠点間の接続装置。
【請求項１７】　第２の拠点を包含する第３の拠点内において未申請のグローバルアドレスが使用されておらず、この第２の拠点では一の端末のみが第１の拠点に対してＶＰＮ接続を行う場合において、
ＶＰＮ接続の際に、第２の拠点が新たに意識する第１の拠点内の端末に対して申請済みグローバルアドレスを別名アドレスとして割り当て、
前記アドレス変換手段はこのアドレスに基づき通信データのアドレスを変換することを特徴とする請求項１２～１６何れか１項記載の複数拠点間の接続装置。
【請求項１８】　前記アドレス変換の際に用いる全ての別名アドレスを予め備えていることを特徴とする請求項１２～１７何れか１項記載の複数拠点間の接続装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は複数の拠点のＶＰＮ接続を支援するための方法及び装置に関するものである。より詳細には、複数の拠点をＶＰＮ接続装置で使用しているアドレスが重複する可能性がある場合に対処するための方法及び装置に関するものである。
【０００２】
【従来の技術】近年、グローバルネットワークで分断された複数の拠点を接続する手段としてＶＰＮ（Virtual Private Network：仮想私設網）が利用されている。ＶＰＮは、後述するＶＰＮトンネリングなどの技術によって実現される。このＶＰＮを用いた通信では、通信データを必要に応じて暗号化している。これにより盗聴や改竄などの可能性があるインターネット等のネットワークを介する通信を、あたかも専用線接続した場合の通信のように安全性を確保して行うことができる。
【０００３】ＶＰＮトンネリングとは、中継装置として機能するＶＰＮ接続装置が、通信データ全体に新たな送信先アドレス及び送信元アドレスを付け、これを相手先のＶＰＮ接続装置に送信する技術である。このとき元のデータは必要に応じて暗号化される。新たに付けられる接続先アドレス及び接続元アドレスは、各拠点のＶＰＮ接続装置のアドレスである。ＶＰＮ接続装置から送出されたデータは、接続先の拠点にあるＶＰＮ接続装置で元の送信元アドレスと送信先アドレスを持つデータに復元される。これにより、各拠点のＶＰＮ接続装置さえグローバルアドレスを持っていれば、このＶＰＮトンネリングを利用することができる。
【０００４】ＶＰＮトンネリングの実装には様々な方法がある。その一つの方法としては、ＶＰＮを利用する両拠点のＶＰＮ接続装置に同一の仮想的なネットワーク（ＶＰＮトンネルと呼ぶ）に接続された仮想インタフェイスを付加し、このＶＰＮトンネルを経由する通信データに対してＶＰＮトンネリングを行うという方法がある。つまり、ＶＰＮ接続装置に付加された仮想インタフェイスを通してＶＰＮトンネルに入る通信データは、ＶＰＮ接続装置により必要に応じて暗号化が行われ、ＶＰＮ接続装置からＶＰＮ接続先の拠点内のＶＰＮ接続装置宛の通信データとして再構成された後、配送される。ここで再構成されたデータは、仮想インタフェイスではなくＶＰＮ接続装置の実インタフェイスを通って相手のＶＰＮ接続装置の実インタフェイスに到着する。このデータを受け取ったＶＰＮ接続装置は、必要に応じて送信元のＶＰＮ接続装置用の暗号鍵を用いて復号化し、元のデータに復元する。ここで、復元されたデータには最初の送信元アドレスと送信先アドレスがついている。このデータは、復元を行ったＶＰＮ接続装置の仮想インタフェイスを経由してＶＰＮ接続装置に入ってきたデータとして扱われる。
【０００５】この方式を使う場合、暗号通信の指定をルーティングの指定として扱うことができるため、アプリケーションにおいて暗号通信のための制御を行わなくて良いことになる。なお、ＶＰＮトンネルの片側が直接クライアントマシン（クライアント端末）に接続されている形態のＶＰＮをエンド・トゥ・ステーション型ＶＰＮと呼び、通常の方式であるステーション・トゥ・ステーション型ＶＰＮと区別する。
【０００６】しかしながら、複数の拠点をＶＰＮなどで相互接続すると、各拠点で使用しているプライベートアドレスが重複する場合がある。この場合、そのまま接続することはできない。これをプライベートアドレスの重複問題と呼ぶ。また、この問題は、接続する拠点同士で使用しているプライベートアドレスが重複しなくても、ある拠点がその拠点を包含する上位の拠点を持っている場合には、上位の拠点を含めて使用しているプライベートアドレスが重複しても発生する。例えば、ある拠点Ａがそれを包含する上位の拠点Ｂで使われているプライベートアドレスを接続先として認識している場合、拠点Ａ

が他拠点Cと接続するときに上位の拠点Bで使用されているアドレスを拠点Cが使用していると、拠点A内のマシンはそのアドレスが示すマシンを特定できなくなってしまう。よって、プライベートアドレスの重複問題は、その拠点が接続先として認識している拠点の中で、その拠点を包含する最上位の拠点において発生するか否かで考えなければならない。

【0007】なお、「グローバルアドレス」とは、インターネットなどのグローバルなネットワークにおいて一意に用意されたマシン識別子である。グローバルアドレス利用のためには然るべき権威に対する申請が必要である。現在のインターネットで使用されているグローバルアドレスは、数の不足の問題が深刻化しつつあり、新たにグローバルアドレスを大量に確保することは困難である。この問題はグローバルアドレスの枯渇問題と呼ばれている。

【0008】また、「プライベートアドレス」とは、利用者が任意に割り当てて使うことができるアドレスである。一般的に、プライベートアドレスを送信元アドレスあるいは送信先アドレスに使用している通信データは、インターネットなどのグローバルなネットワークに直接流出することが禁止されている。但し、後述するVPNトンネリング等の技術によって、新たに送信元あるいは送信先アドレスとしてグローバルアドレスを付加することによりプライベートアドレスが隠蔽されるのであれば、このようなデータがグローバルネットワークに流出することは許される。

【0009】また、「拠点」とは、複数の端末が接続されたネットワークあるいはサブネットワーク又は1台の端末のことを指す。LANやイントラネットがその例である。各拠点では、プライベートアドレスに基づくアドレス体系で独自に端末やホストマシンを管理している場合がある。

【0010】従来、前述したようにVPN接続の際などに生じるプライベートアドレスの重複問題に対しては、以下のような方法が採られてきた。

【0011】(A)外部接続性の放棄

VPN接続をしている間、自拠点内のマシンは接続先拠点内のマシン以外とは接続が行われないようにする。

【0012】(B)アドレス付け替え

少なくとも一つの拠点のアドレスを拠点間で重複しないように付け直す。

【0013】(C)グローバルアドレスの付け替え

前記(B)の場合において、付け直すアドレスとしてグローバルアドレスを使用する。この方法では、一度グローバルアドレスを付けた拠点が、それ以降さらに多重にVPN接続を行う際にはアドレス衝突の問題を起こさない。その点で、この方法は(A)よりも優れているといえる。ここで「ある拠点(以後、拠点Aと呼ぶ)が多重にVPN接続する」とは、拠点Aが複数の拠点B～Zと同時にVPN接続することを意味する。このとき、拠点Aに対してVPN接続している別拠点B～Z間において、相手拠点に属しているマシン同士の接続が可能である必要はない。

【0014】(D)アドレス変換装置による非共通別名アドレス利用

拠点間の接続境界点にアドレス変換装置を設置し、別名アドレスを利用する。別名アドレスは、お互いの拠点におけるアドレス体系の中で各拠点の管理者が相手の拠点にあるマシンのアドレスに対して用意し、アドレス変換装置に登録しておく。自拠点内では相手のアドレスとして別名アドレスを使用し、通信データが相手の拠点に入る際にアドレス変換装置により、通信データの送信先アドレスとして使用された別名アドレスを実際のアドレスに変換する。このとき同時に、送信元アドレスを送信先の拠点における別名アドレスに付け替える。

【0015】(E)アドレス変換装置による共通別名アドレス利用

接続を行う拠点間で重複しないアドレスを確認して共通の別名として前記(D)と同様に運用する。前記(D)の場合よりも管理が楽になるという利点を有している。

【0016】(F)アドレス変換装置なしの共通別名アドレスの利用

前記(D)の場合で、接続を行う拠点内のマシンそのものが別名アドレスを直接扱うことができるようにする。前記(D)と違い、アドレス変換装置は使用しない。相手の拠点のマシンと接続するときには別名アドレスを使用する。

【0017】(G)別名アドレスとしてグローバルアドレスの利用

前記(C)(D)(E)の場合で、別名アドレスとして正規に取得したグローバルアドレスを用いる。接続の準備の際に各拠点のアドレスの情報を参照する必要がないという特徴を持つ。

【0018】

【発明が解決しようとする課題】本発明は、以下の課題を全て解決することを目的としている。以下の課題は、従来の方法で部分的に解決されている場合もあるが、全てを同時に解決するような方法は、本発明を除いて存在しない。

【0019】課題1．接続性確保

VPN接続を行う2つの拠点内のマシンが、VPN接続前に通信可能な全てのマシン(拠点外のマシンを含む)と、VPN接続後も接続可能に維持する手段を提供する。前記(A)の方法はこの条件を満たさない。

【0020】課題2．アドレス付け替えの回避

前記(B)(C)の方法では、アドレスの付け替え作業には一般に大きな手間がかかる。また、既に運用されているネットワークの場合は変更が事実上できない場合が多いため、現実的な方法ではない。そこで、従来使用し

ていたアドレスを使い続けることができる手段を提供する。

【００２１】課題３．片側拠点の管理情報の非利用

前記（Ｄ）（Ｅ）（Ｆ）の方法において、プライベートアドレスの範囲内で別名アドレスを用意するという作業は、拠点内の管理方針と矛盾を起こさないようにする必要がある。このため管理者の権限を持つものが判断することが望ましいが、これは一般的に手間がかかるものである。そこで、少なくとも片側の拠点内の管理方針は参照しなくても済む手段を提供する。

【００２２】課題４．アドレス交渉の回避

前記（Ｅ）（Ｆ）の方法では、ＶＰＮ接続に先立ち、接続する複数の拠点が持つアドレス体系の中で重複しない範囲を特定する必要がある。この特定のためには行う交渉は一般に手間がかかるものである。そこで、このような交渉作業なしで接続を確立する手段を提供する。

【００２３】課題５．多重接続時の再設定の回避

前記（Ｂ）（Ｅ）（Ｆ）の方法では、さらに別の拠点を接続する場合、先の２つの拠点では重複しなかったアドレスが新たに重複する場合がある。この場合、新たに重複しないアドレスを用意し接続ホストの別名アドレスを用意し直す必要がある。この作業は一般に手間のかかるものである。そこで、従来のＶＰＮ接続環境の再設定をすることなく新たなＶＰＮ接続が可能な手段を提供する。

【００２４】課題６．アドレス情報の非開示

前記（Ｂ）（Ｄ）（Ｅ）（Ｆ）の方法では、ＶＰＮ接続を行う際に互いの拠点のアドレス情報を提供する必要がある。これはセキュリティ上好ましくないものである。そこで、互いの拠点のアドレス情報を提供することなくＶＰＮ接続が可能な手段を提供する。

【００２５】課題７．片側拠点の設定の簡易化

前記（Ｂ）（Ｄ）（Ｅ）（Ｆ）（Ｇ）の方法では、ＶＰＮ接続を行う拠点の双方において、ＶＰＮ接続のために必要になるアドレスに関する手続（自拠点内ＶＰＮ接続装置に追加される仮想インタフェイスへのアドレス付け、相手拠点内マシンの別名アドレスの用意など）が必要である。そこで、ＶＰＮ接続を行う拠点のうち、片側の拠点がＶＰＮ接続のために必要になるアドレスに関する手続を行えばＶＰＮ接続が可能な手段を提供する。これは片側をユーザであると考えた場合、ユーザの負担を減らすことを意味する。また、これは前記課題６を包含するものである。

【００２６】課題８．グローバルアドレス大量消費の回避

前記（Ｃ）（Ｇ）の場合、ＶＰＮを経由して接続するマシンの数のグローバルアドレスが必要になる。したがって、マシン数が多くなる場合、現在のインタネットのアドレス体系（ＩＰｖ４）におけるグローバルアドレスの大量取得は困難であるという理由からこの方法の実現は困難になる。そこで少数のグローバルアドレスの使用でＶＰＮ接続が可能な手段を提供する。

【００２７】課題９．接続拠点増加時のグローバルアドレス消費量増加の回避

前記課題８において、さらに、拠点Ｓが複数の拠点に対して多重にＶＰＮ接続を行う際に、拠点Ｓから見た接続先拠点数の増加に対して、使用するグローバルアドレスの数が増加しない手段を提供する。

【００２８】

【課題を解決するための手段】本発明は、従来の方法（Ｄ）の「アドレス変換装置による非共通別名アドレス方式」を基本として採用し、これを拡張したものである。従来の方法（Ｄ）を基本として採用することにより、課題１（接続性確保）、課題２（アドレス付け替えの回避）、課題４（アドレス交渉の回避）、課題５（多重接続時の再設定の回避）は達成される。また、方法（Ｄ）には、課題８（グローバルアドレス大量消費の回避）、及び課題９（接続拠点増加時のグローバルアドレス消費量増加の回避）は直接関係しないことになるのだが、本方法では後述するようにグローバルアドレスを使用するため、検討を要する。

【００２９】本発明が、方法（Ｄ）を元にしているにも拘わらず、本願で他の方法の問題点を上げている理由は、方法（Ｄ）の拡張を行うにあたって、他の方法の問題点を持ち込まないことを明記するためである。

【００３０】また、本発明で採用するＶＰＮの方式は、第２の拠点と第１の拠点とをエンド・トゥ・ステーション型で接続する。したがって、すなわち第２の拠点であるクライアント拠点側のマシン（端末）のうち、ＶＰＮトンネルを経由して接続を行うものは、ＶＰＮトンネルごとに１台のみである。そのマシンは、ＶＰＮトンネルの仮想インタフェイスが付加されたクライアントマシンそのものである。通信データの送信元として使用されるアドレスは、データが出力されるインタフェイスのアドレスであるため、ＶＰＮトンネルの内部を通過する通信データのうち、クライアント側のマシンを表すものとして使われるアドレスは、仮想インタフェイスのアドレスだけになる。また、また、第１の拠点であるサーバ側拠点は、複数のマシンが接続されたＬＡＮである。

【００３１】本発明では、前記（Ｄ）の方法に加えてさらに２つの工夫を行う。この２つの工夫が、本発明の本質である。以下、その内容を説明する。

【００３２】第１の工夫は、ＶＰＮ接続時にクライアントが新たに認識するアドレスとしてグローバルアドレスを使うという方法である。ＶＰＮ接続を行うと、ＶＰＮ接続を行うマシンは、接続前から使用しているアドレスに加えて、新たなアドレスを認識することになる。それは、ＶＰＮトンネルの両端となる仮想インタフェイスのアドレス２つと、クライアントが接続を行う第１の拠点であるサーバ拠点内のマシンのアドレスである。前記

（Ｄ）の方式を使うと、クライアント側で新たに認識するアドレスとサーバ拠点側で意識するアドレスは異なることになる。そのうちのクライアント側で認識するアドレスだけでグローバルアドレスを使用し、サーバ側では、前記（Ｄ）の方法と同じくサーバ拠点側のプライベートアドレスを割り振る。ここで使用されるグローバルアドレスは、グローバルネットワーク内でのルーティングで使用されるものではなく、あくまで、ＶＰＮの内側のみで使用されるアドレスである。

【００３３】この第１の工夫により、前記課題３、６及び７が解決する。その理由を以下に説明する。

【００３４】まず、課題３（片側拠点の管理情報の非利用）が解決される理由を説明する。この工夫では、第２の拠点であるクライアント拠点が新たに認識するアドレスとしては、グローバルアドレスだけになるようにする。グローバルアドレスはクライアント側の拠点内で使用されるプライベートアドレスと重複することはありない。よってクライアント拠点にいるユーザがアドレス変換装置の動作設定の際に、クライアント側で使用していないプライベートアドレスの情報を入力することや、クライアント拠点内のマシンのうち、ＶＰＮを経由して通信を行うマシンのアドレス（プライベートアドレス）を入力する必要はない。これにより課題３が解決される。

【００３５】次に、課題６（アドレス情報の非開示）が解決される理由について説明する。開示すべきではないアドレス情報とは、各拠点内で使用されているプライベートアドレスの情報である。本方法を使った場合、第２の拠点であるクライアント拠点で必要な設定は、クライアントのＶＰＮ接続装置と第１の拠点であるサーバ拠点のＶＰＮ接続装置のＶＰＮ接続を確立するためのものだけでよい。このときにクライアント側として使用されるアドレスは、クライアント拠点側のファイアウォールで使用されるアドレスであり、サーバ拠点でもファイアウォール上にあるＶＰＮサーバのアドレスである。このアドレスは、ＶＰＮトンネリングによってカプセル化された後に付加されるアドレスとして使われる。設定の際に、クライアント拠点内のプライベートアドレスの情報を求められることはないので、この情報の流出は避けられる。ここで、サーバ拠点からクライアントマシンへのＶＰＮトンネル内を経たアクセスは、クライアントマシンのプライベートアドレスではなく、クライアント側の仮想インタフェイスのアドレスが使用される。また、サーバ拠点では、クライアントのアドレスとしてグローバルアドレスを意識するのではなく、各クライアントにサーバ拠点で使用しているプライベートアドレスを割り当てることになる。しかし、この割り当ては、サーバ拠点側に設置された装置への設定だけで済む。よってその情報はクライアント拠点に知らされないため、アドレス情報は流出しない。

【００３６】課題７（片側拠点の設定の簡易化）を達成するために、本方法では、クライアントが認識するアドレスとしてのグローバルアドレスをサーバ拠点側で予め用意する。そして、エンド・トゥ・ステーション型ＶＰＮの特徴として、第２の拠点であるクライアント側の仮想インタフェイスのアドレス割り当てを、第１の拠点であるサーバ拠点側から行うことができるため、これを利用する。

【００３７】第２の工夫は、複数のマシンを示すものとして同一のグローバルアドレスを利用することである。つまり、複数のクライアント拠点が認識するアドレスとして、そのアドレスが互いに別のマシンを示すものであっても、同じアドレスの組を使用するのである。

【００３８】この第２の工夫により、課題８（グローバルアドレス大量消費の回避）及び課題９（接続拠点増加時のグローバルアドレス消費量増加の回避）が解決される。

【００３９】

【発明の実施の形態】（第１の実施の形態）以下に、本発明の第１の実施の形態にかかる複数拠点間の通信について図１を参照して説明する。図１はネットワーク構成図である。なお、図において、実アドレスについては「＜＞」を付すとともに、別名アドレスについては「（）」を付すことにより両者を区別している。また、図において、実線矢印は接続要求が存在する組を表し、点線はＶＰＮトンネルを表している。

【００４０】図１に示すように、第１の拠点１００と第２の拠点２００－１～２００－ｎは、例えばインターネット等のグローバルアドレスに基づくネットワーク１を介して接続されている。そこで本実施の形態では、このネットワーク１を利用して第１の拠点１００と複数の第２の拠点２００－１～２００－ｎの間にそれぞれＶＰＮを構築し、第１の拠点１００と第２の拠点２００－１～２００－ｎ間で通信を行うものである。なお、第２の拠点２００－１～２００－ｎは、それぞれ第３の拠点３００－１～３００－ｎに包含されている。例えば、第３の拠点と第２の拠点との関係が一のネットワークとそのサブネットワークという関係になっている場合である。

【００４１】ここで、ＶＰＮ接続は、前述したエンド・トゥ・ステーション型である。すなわち、第２の拠点２００－１～２００－ｎ内のクライアントマシン２０１（クライアント端末）はそれぞれ１台のみ設置されている（図１の２０１－１～２０１－ｎ）。また、各拠点２００－１～２００－ｎのクライアントマシン２０１－１～２０１－ｎはそれぞれＶＰＮ接続機能部２０２－１～２０２－ｎが実装されている。各クライアントマシン２０１－１～２０１－ｎは、独自のプライベートアドレスＰＡＣ１～ＰＡＣｎを有している。また、各クライアントマシン２０１－１～２０１－ｎは、前記プライベートアドレスの他にグローバルアドレスＧＡＣ１～ＧＡＣｎを有している。第２の拠点２００のそれぞれには、クラ

イアントマシン２０１のプライベートアドレスをグローバルアドレスに変換するためにＰＲＯＸＹサーバやファイアウォールなどのアドレス変換部（図示省略）を有している。これにより、第２の拠点２００はネットワーク１と直接通信し、ＶＰＮを構築可能としている。なお、各クライアントのプライベートアドレスは、複数の第２の拠点２００間で重複していてもよい。

【００４２】第１の拠点１００には、主装置１１０内に１つのＶＰＮ接続機能部１１１が設けられている。このＶＰＮ接続機能部１１１は独自のプライベートアドレスＰＡＳ０を有する。また、このＶＰＮ接続機能部１１１はこのプライベートアドレスＰＡＳ０の他にグローバルアドレスＧＡＳ０を有している。これによりネットワーク１と直接通信し、ＶＰＮを構築可能としている。また、この主装置１１０にはアドレス変換機能部１１２が設けられている。

【００４３】また、第１の拠点１００には、主装置１１０に複数のマシン１０１－１～１０１－ｎがＬＡＮを介して接続している。各マシン１０１－１～１０１－ｎは、それぞれプライベートアドレスＰＡＳ１１～ＰＡＳ１ｎを有している。これらのプライベートアドレスＰＡＳ１１～ＰＡＳ１ｎは、第２の拠点２００の各クライアントマシン２０１－１～２０１－ｎのプライベートアドレスＰＡＣ１～ＰＡＣｎと重複していてもよい。

【００４４】以下、第１の拠点１００と第２の拠点２００間における通信の基本手順について説明する。なお、以下において、アドレスを表す記号としてＰＡで始まるものはプライベートアドレスを表すものとし、ＧＡで始まるものはグローバルアドレスを表すものとする。

【００４５】（１）ＶＰＮ接続準備

まず、ＶＰＮ接続の準備として、第２の拠点２００－１～２００－ｎのＶＰＮ接続機能部２０２－１～２０２－ｎを、第１の拠点１００の接続機能部１１１が接続要求を受ける対象として予め登録しておく。以下、第１の拠点１００内のマシン１０１－１と第２の拠点２００－１内のマシン２０１－１間の通信を例にとって説明する。

【００４６】第１の拠点１００は、ＶＰＮ接続後のクライアントマシン２０１－１の仮想インタフェイスに割り振る別名アドレスＰＡＳ３１と、第１の拠点１００のＶＰＮ接続機能部１１１に付加される仮想インタフェイスの実アドレスＰＡＳ２１を用意する。これはどちらも第１の拠点１００内のプライベートアドレスである。

【００４７】ここで、アドレスの割り振りには登録時に静的に割り振る方法と、ＶＰＮ接続確立時に動的に割り振る方法の２つがあり、本発明ではどちらであるかは限定しない。ここでは前者の静的に割り振るものとする。また、この時、必要であれば暗号鍵の準備を行う。片側で用意した暗号鍵で暗号化されたデータが、もう片側で用意した暗号鍵で復号化することが可能であるようにしておく。本方法では、この暗号鍵が共通なものであるか非共通なものであるかは限定しない。

【００４８】また、本発明では各クライアントマシン２０１－１～２０１－ｎごとに第１の拠点１００内のマシン１０１－１～１０１－ｎの別名アドレス用のグローバルアドレスを実際の第１の拠点１００内のマシン１０１－１～１０１－ｎに対応づける必要がある。ここではクライアントマシン２０１－１がマシン１０１－１に接続要求を持っていることになっているので、グローバルアドレスＧＡ１を、マシン１０１－１の実アドレスＰＡＳ１１に対応づけるように設定する。この設定はアドレス変換機能部１１２の動作に反映される。

【００４９】さらに、後述するアドレスの割り当て時に用いるグローバルアドレスＧＡ２及びＧＡ３を予め用意しておく。前記グローバルアドレスＧＡ１、グローバルアドレスＧＡ２及びＧＡ３は、第１の拠点１００で使用するものとして所定の権威（例えばグローバルネットワークがインターネットならばＮＩＣ）に申請済みの範囲内のもを使用するのが好ましい。これにより、第２の拠点２００において、クライアントマシン２０１が第１の拠点１００以外に接続する際に、当該他の接続先とグローバルアドレスの重複を起こすことがない。

【００５０】（２）接続要求の発行

以降は第２の拠点２００－１内のクライアントマシン２０１－１から第１の拠点１００内のマシン１０１－１へ接続を行う際の処理の流れについて説明する。まず、クライアントマシン２０１－１のＶＰＮ接続機能部２０２－１が、第１の拠点１００のＶＰＮ接続機能部１１１に接続要求を発行する。

【００５１】（３）クライアントの認証

ＶＰＮ接続機能部１１１はクライアントマシン２０１－１が登録されたクライアントマシンであることを確認するための認証を行う。

【００５２】（４）ＶＰＮ接続の確立

ＶＰＮ接続機能部２０２－１及びＶＰＮ接続機能部１１１はクライアントマシン２０１－１と第１の拠点１００との間のＶＰＮ接続を確立する。これは仮想インタフェイス及びＶＰＮトンネルを利用可能な状態にすることを指す。

【００５３】この時に必要なアドレスは、第１の拠点１００側のＶＰＮ接続機能部１１１に予め登録してあるものを使用する。このアドレスは、第１の拠点１００側のＶＰＮ接続機能部１１１に付加される仮想インタフェイス用の実アドレスとしてＰＡＳ２１、その別名アドレスとしてＧＡ２、クライアントマシン２０１－１側のＶＰＮ接続機能部２０２－１に付加される仮想インタフェイス用の実アドレスとしてＧＡ３、その別名アドレスとしてＰＡＳ３１の計４つになる。このように本方法では、クライアントに付加される仮想インタフェイスの実アドレスは第１の拠点１００ごとに共通のグローバルアドレスＧＡ３を使用し、第１の拠点１００のＶＰＮ接続機能

部１１１の仮想インタフェイスに付加されるアドレスとしては、予め前記（１）において登録してあるものを使用する。

【００５４】以上で、第１の拠点１００と第２の拠点２００－１間でＶＰＮが構築された。以降は、クライアントマシン２０１－１がＶＰＮトンネルを介して第１の拠点１００内のマシンと通信を行う過程について説明する。

【００５５】（５）クライアントマシンから第１の拠点１００内マシンへの通信データの送信

クライアントマシン２０１－１から第１の拠点１００内のマシン１０１－１への通信を行う。この時、通信データはＶＰＮトンネルを経由して第１の拠点１００内のマシンへ向かう。クライアントマシン２０１－１で生成され、はじめにＶＰＮトンネルに出されるデータには仮想インタフェイスのアドレスＧＡ３が送信元アドレスとして付加される。このアドレスは上で示したように、第１の拠点１００にとってはクライアントマシンによらず固定のグローバルアドレスである。このデータの送信先アドレスにはマシン１０１－１の別名アドレスであるグローバルアドレスＧＡ１が使用される。ここで、このアドレスは、前記（１）でマシン１０１－１に対応づけられたグローバルアドレスである。

【００５６】（６）接続先の振り分け

第１の拠点１００にある主装置１１０内のアドレス変換機能部１１２では、ＶＰＮトンネルを経由して仮想インタフェイスから入ってきた通信データの送信先アドレス及び送信元アドレスを、第１の拠点１００内で使用されるプライベートアドレスに変換する。アドレス変換機能部１１２は、各クライアントマシンが接続するマシンのアドレスを管理しており、適切な送信先にアドレスを付け替えることによって接続先を振り分ける。この時、各クライアントマシンごとに個別のＶＰＮトンネルを使用することになっているので、データが経由する仮想インタフェイスによってどのクライアントから来たデータであるかを認識する。クライアントマシン２０１－１からの通信データの場合、送信先アドレスＧＡ１をＰＡＳ１１に変換する。クライアントマシンが接続するマシンの数が第１の拠点１００内に複数ある場合は、変換前の送信先アドレスにしたがい接続先を特定する。また、送信元アドレスは前記（１）でクライアントの登録の際に用意した、第１の拠点１００内で使用するクライアントの別名アドレスに変更する。クライアントマシン２０１－１からの通信データの場合、送信元アドレスはＧＡ３からＰＡＳ３１に変換される。

【００５７】（７）クライアントマシンに向けての通信

第１の拠点１００内のマシンから、第２の拠点のクライアントマシンに向けての通信に対しては、前記（６）で示しアドレス変換の逆を行うようにする。この時、クライアントマシンにつけられた第１の拠点１００内のアドレスを送信先アドレスとして持つ通信データが、そのクライアントマシンに接続されたＶＰＮトンネルを経由するようになっていなければならない。これは、第１の拠点１００内のデータ配送制御機構により実現すればよい。

【００５８】（第２の実施の形態）次いで、本発明の第２の実施の形態にかかる複数拠点間の通信について図２及び図３を参照して説明する。図２はネットワークの接続要求を説明する概念図、図３はネットワーク構成図である。なお、第１の実施の形態と同一の要素については同一の符号を付した。

【００５９】本実施の形態では、図２に示すように、第２の拠点２００－０内の複数のクライアントマシン２０１－０１～２０１－０ｍがＶＰＮを経由して第１の拠点１００内のマシン１０１－１に接続したいという要求がある場合について説明する。

【００６０】このような接続形態についても、以下に示す手順により、図３のようにネットワーク構成を変更すれば、クライアントマシン側の拠点中のマシンの数を一つに抑え前記図１の基本構成に当てはめることができる。これにより前記課題８を解決する。

（１）クライアントマシン２０１－０１～２０１－０ｍの全てにＶＰＮ接続機能部装置２０２－０１～２０２－０ｍを内蔵させる。

（２）クライアントマシン２０１－０１～２０１－０ｍの各マシンに対し、それぞれ１台のみを構成要素とする部分拠点２１０－０１～２１０－０ｍがあると考える。

（３）部分拠点２１０－０１～２１０－０ｍから第１の拠点１００に対して個別のＶＰＮを構築する。

【００６１】（第３の実施の形態）次いで、本発明の第３の実施の形態にかかる複数拠点間の通信について図４を参照して説明する。図４はネットワーク構成図である。なお、第１及び第２の実施の形態と同一の要素については同一の符号を付した。

【００６２】本実施の形態では、第２の実施の形態と同様に、第２の拠点２００－０内の複数のクライアントマシン２０１－０１～２０１－０ｍがＶＰＮを経由して第１の拠点１００内のマシン１０１－１に接続したいという要求がある場合について説明する。

【００６３】図４に示すように、第２の拠点２００－０にＶＰＮ接続装置２０２－０を設置し、ＶＰＮ接続装置２０２－０と第１の拠点１００の主装置１１０の間でＶＰＮ接続を行う。ここで、ＶＰＮ接続装置２０２－０はクライアントマシン２０１－０１～２０１－０ｍからの通信データの送信元アドレスを自分のアドレスに置き換える機能を持つ変換部２２０を内蔵するものとする。インターネットの世界においてこの技術は「ＩＰマスカレード」又は「ＮＡＰＴ」等と呼ばれる。これにより第１の拠点１００から見た場合、クライアントマシン２０１－０１～２０１－０ｍからの全ての通信は、ＶＰＮ接続

装置２０２－０からの通信であるように見える。クライアントマシン２０１－０１～２０１－０ｍにはそれぞれ、第３の拠点３００－０のプライベートアドレスＰＡＣ０１～ＰＡＣ０ｍがついているとすると、最初にこのアドレスを送信元アドレスとしている通信データが、ＶＰＮ接続装置２０２－０を通過する際、送信元アドレスとして、ＶＰＮ接続装置２０２－０のアドレスＧＡ３に置き換わる。さらに、このアドレスは図１に示したものと同じく、主装置１１０のアドレス変換機能部１１２を通過する際に、別名アドレスＰＡＳ３０に置き換わる。このＰＡＳ３０は第１の拠点１００のプライベートアドレスである。このように、ＶＰＮ接続装置２０２－０だけからなる拠点２００－００を第２の拠点として考えることによっても図１の構成に置き換えることができる。この方法で課題８を解決することができる。同様の方法は、クライアント側である第２の拠点に限らず、サーバ側の第１の拠点においても使うことができるが、ここでは省略する。

【００６４】（第４の実施の形態）次いで、本発明の第４の実施の形態にかかる複数拠点間の通信について図５を参照して説明する。図５はネットワーク構成図である。なお、前述した各実施の形態と同一の要素については同一の符号を付した。

【００６５】本実施の形態では、第２の拠点２００－１が第１の拠点１００内の複数のマシン２０１－１及び２０１－２に接続を行う場合を示す。この場合にはＶＰＮトンネルを経由して接続するマシンの数だけグローバルアドレス（ＧＡ１１，ＧＡ１２の２つ）が必要になる。第１の拠点１００内のマシンの別名アドレスとして使用されるグローバルアドレスの総数は、第１の拠点１００に接続する第２の拠点２００－１～２００－ｎの中で、同時に接続を行う第１の拠点１００内のマシンの総数の最大値になる。ここで、この数はクライアント側拠点である第１の拠点２００の数そのものには影響を受けない。したがって、依然として課題９は解決されている。すなわち、例えば図５に示すように、第２の拠点２００－２が第１の拠点１００内のマシン１００－２と接続する場合には、このマシン１００－２に割り当てる別名アドレスとして、グローバルアドレスＧＡ１１を用いることができる。つまり、第２の拠点２００－１と第１の拠点１００の接続用に用いた別名アドレスと同一のアドレスを、第２の拠点２００－２と第１の拠点１００の接続時にも用いることができる。

【００６６】（第５の実施の形態）次いで、本発明の第５の実施の形態にかかる複数拠点間の通信について図６を参照して説明する。図６はネットワーク構成図である。なお、前述した各実施の形態と同一の要素については同一の符号を付した。

【００６７】本実施の形態では、第１の拠点１００に接続する第２の拠点２００－１と第２の拠点２００－２が相互に通信を行う場合を示す。この場合には、第２の拠点２００－１から見ると第２の拠点２００－２内のクライアントマシン２０１－２は第１の拠点１００に存在しているように見える。逆に第２の拠点２００－２から見た場合、第２の拠点２００－１内のクライアントマシン２０１－１が第１の拠点１００に存在しているように見える。この場合、お互いに相手のアドレスとして同じアドレスＧＡ１を意識することになる。

【００６８】また、異なるＶＰＮ方式に対応した主装置１００を複数用意することにより、異機種間ＶＰＮ通信が可能になる。

【００６９】

【発明の効果】現在のインターネットのアドレス体系（ＩＰｖ４）においてグローバルアドレス不足の問題は深刻なものとして考えられている。十分なグローバルアドレスを持つ新たなアドレス体系（ＩＰｖ６）への以降の検討が進められているが、この新たなアドレス体系が主流に使われるようになるまでには、まだ時間がかかると考えられている。しかも、現在使用されているアドレス体系がインターネット上で使われなくなることはなく、将来的にも共存環境が続くと言われている。

【００７０】一方、アドレスが大量に利用できるという環境にあれば、コンピュータネットワークの使用方法も変わってくると考えられる。例えば一台のホストマシンを仮想的に複数台に見せる技術などにより、小規模な環境を大量に扱うことなどが可能になる。この場合アドレスも大量に消費することになる。また、１台のマシンが複数のネットワークに仮想的に接続されるという形でエクストラネットを構築するということも考えられる。本発明は、このような形態のエクストラネット構築を考慮に入れている。この場合、１台のマシンで複数のアドレスを使用することになり、ネットワーク全体としてはやはりアドレスが大量に必要になる。このようにこれらの実現の際にはグローバルアドレスの枯渇問題が大きな障害になっているのである。

【００７１】グローバルアドレス枯渇問題の対策としてプライベートアドレスが各拠点内で広く使われつつある。しかし近年のエクストラネットの発展に伴い、複数の拠点をＶＰＮ接続する状況が増えてきており、この際に発生するプライベートアドレスの重複問題が深刻化することになった。従来、この問題を解決するためには多大な設定の手間がかかっていた。

【００７２】前述したように、本発明では、ＶＰＮ接続の関係に関して接続拠点の役割をサーバ側である第１の拠点とクライアント側である第２の拠点に分け、第１の拠点に本発明の装置を設置することによって、プライベートアドレスの重複を起こす可能性のあるＶＰＮ接続の際に、第２の拠点側の設定負担を軽減することを可能にする。

【００７３】これは、グローバルアドレスを別名アドレ

スとして利用することにより、アドレス重複を回避するという手法と、限られた少数のグローバルアドレスを無制限に多数のクライアント拠点との接続のために使うという手法により実現される。

【００７４】また、サーバ側である第１の拠点でプライベートアドレスを使う代わりにＩＰｖ６のアドレス体系の下でアドレス付けを行うことにより、現在のアドレス体系と新たなアドレス体系の共存関係を実現できる。よって実施例に示したサーバレンタルサービスにおいてＩＰｖ４とＩＰｖ６の共存環境をこの方法により構築することができる。このようなサービス対象者として現在のアドレス体系の拠点をサポートする限り本発明は有用であるといえる。

【００７５】本発明には以下のような利用例が考えられる。

【００７６】例１．サーバレンタルサービス

各種サーバや電子掲示板やファイル共有環境などをネットワーク上で提供する。通信経路の安全性はＶＰＮによって確保する。複数の企業に属するマシンをクライアントとして接続し、エクストラネットを簡単に実現することができる。

【００７７】利点としては、レンタルという形態をとることで、初期投資のコストが少なくて済むということ、必要になったときにすぐに利用できること、短期間での運用が可能であること、サーバの管理をサービスの提供者に委託可能であることなどがある。また、企業のファイアウォールの設定は内側から外側への接続は許可される場合が多いので、エクストラネット環境の構築をより簡単に行うための手段になりうる。

【００７８】このサービスとを大規模に行う際に、グローバルアドレスの枯渇問題及びプライベートアドレスの重複問題を解決することが必要になってくる。本発明を利用すれば、クライアント側の設定の負担が少ない形でこの問題を解決できる。

【００７９】例２．企業内サーバ集中管理センタ

本方式を利用して、企業内でアプリケーションの集中管理センタを構築する。集中管理センタを構築する利点は、企業内で分散していたアプリケーション環境を集中管理することによりＴＣＯ（Total Cost of Ownership：所有に由来する総コスト）を削減することなどがある。例えばソフトウェアのアップグレードに要するコストを抑えることや、重要な情報を守るための機器設置環境を充実させるためのコストを抑えること、システムの管理技術を持つ人材を集中することによって人的コストを削減することなどがある。

【００８０】企業内でも他部署に流出を避けたい情報を扱う場合も考えられるので部署単位で暗号通信を使ったＶＰＮを利用することはあり得るためＶＰＮの利用は有用である。また、部署間にまたがったグループを構成する際のネットワーク環境を提供するためにも、ここに示す集中管理センタは有用である。

【００８１】本発明を利用することによって、各部署間でプライベートアドレスが重複するような使い方をしている場合でも集中管理が可能になる。

【００８２】例３．アプリケーションサーバレンタルサービス

従来のアプリケーションの流通形態は、アプリケーションをパッケージとして販売し顧客が自分のマシンにインストールして使うという形をとっていた。本発明を利用し、ネットワークを経由してサービスセンタ内のサーバ機に顧客がアクセスすることによって利用できるようにすることを考える。このサービスの利点としては、使用度数に応じた従量課金など料金徴収の方法に多様性を持たせることができることや、クライアント側の設備変更が最小限で済むことなどがある。本発明は安全な通信の確保のためにＶＰＮを利用しているため使用プロトコルの制限が少ないという特徴がある。なお、このサービスも例１と同様の問題を持っており、本発明によってこれらが解決される。

【００８３】例４．ＶＰＮ接続中継システム

ＶＰＮ接続の要求がある複数の拠点が、中継システムを介して接続を行うことを考える。本発明におけるサーバ側拠点である第１の拠点は、ここで言う中継システムとして機能し、クライアント側拠点である第２の拠点のＶＰＮ接続の中継を行う。中継センタが有用になる場合としては、プライベートアドレスの重複問題を解決する手段としてこの中継システムを使う場合や、ファイアウォール越え問題などにより、接続拠点のうち一つもＶＰＮ接続の待ち受けができない場合や、各拠点のネットワーク情報を開示せずに接続を行う場合などがある。

【００８４】但し、本方法は第２の拠点に１台のクライアントマシンしかないことを前提とするので、接続先としてクライアントマシン１台ではなくそのクライアントマシンの属する上位拠点のマシンへのアクセスを考えるときは、図４のように、他のマシンをあたかもそのクライアントであるかのように見せるＩＰマスカレード機能などが必要になる。

【００８５】例５．異種暗号方式中継システム

前記例４で示した実施例において、サーバ側拠点である第１の拠点に異なるＶＰＮ方式をもとにした複数の主装置を設置することにより、異なる方式のＶＰＮ接続装置を持つ拠点を接続するための中継システムとなることができる。

【図面の簡単な説明】

【図１】ネットワーク構成図

【図２】ネットワークの接続要求を説明する概念図

【図３】ネットワーク構成図

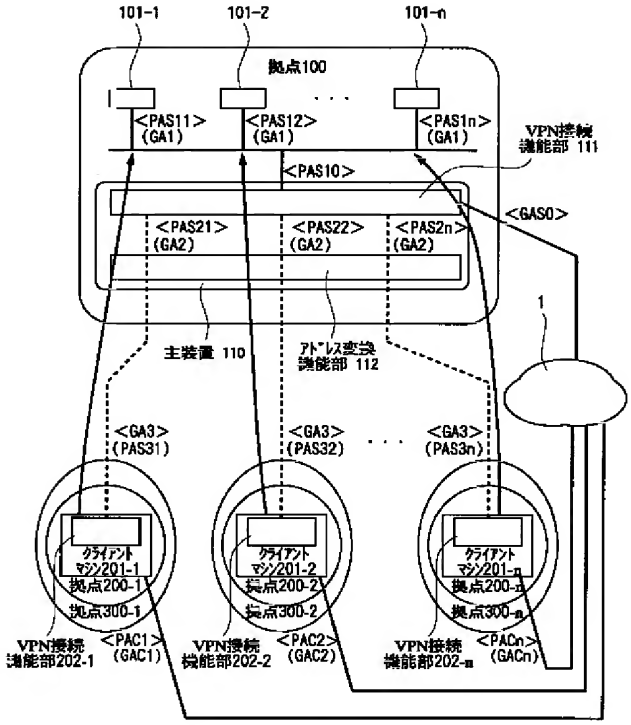
【図４】ネットワーク構成図

【図５】ネットワーク構成図

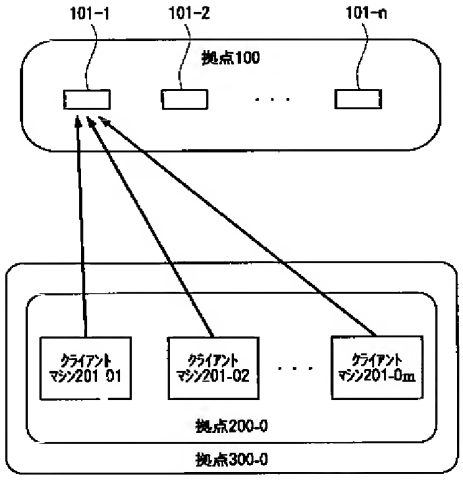
【図６】ネットワーク構成図

【符号の説明】
1…ネットワーク、100…第1の拠点、101…マシン、110…主装置、111…VPN接続機能部、112…アドレス変換機能部、200…第2の拠点、201…クライアントマシン、202…VPN接続機能部

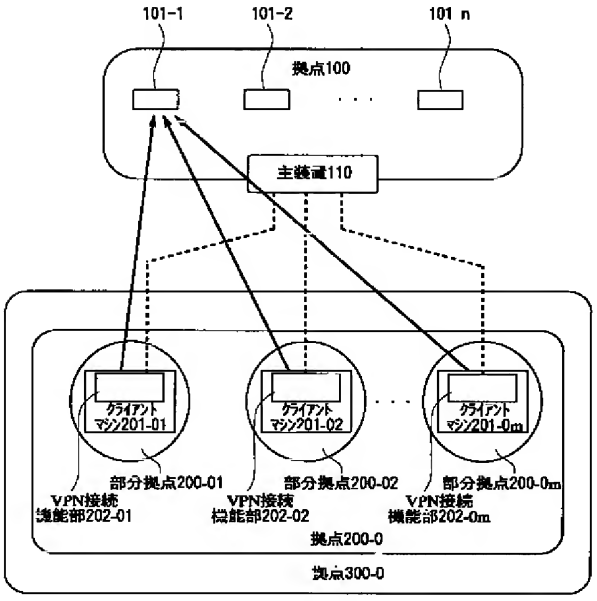
【図1】



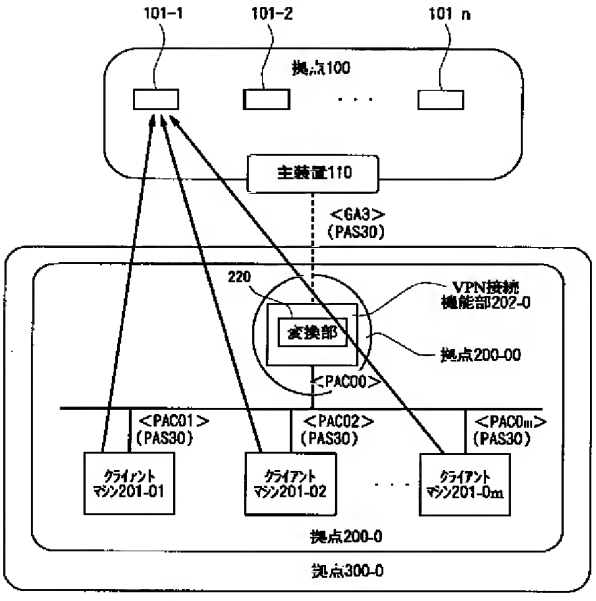
【図2】



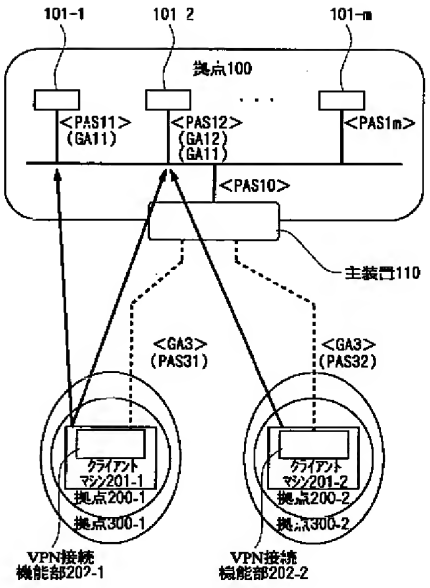
【図3】



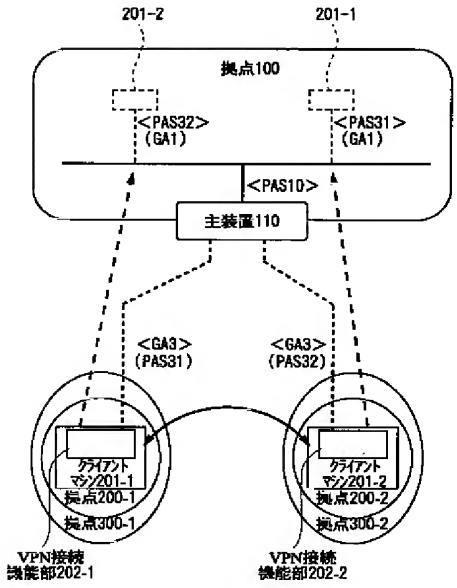
【図4】



【図5】



【図6】



フロントページの続き

Fターム(参考) 5K030 GA15 GA19 HC01 HD09 LB05
LD16 LD17
5K033 AA04 AA08 AA09 CB09 DA06
EC03
9A001 BB02 BB03 BB04 CC03 CC07
CC08 DD12 EE02 EE03 JJ18
JJ27 KK56 LL03